View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Journal of Discrete Algorithms 5 (2007) 436–454

JOURNAL OF DISCRETE ALGORITHMS

www.elsevier.com/locate/jda

A station strategy to deter backoff attacks in IEEE 802.11 LANs

Jerzy Konorski *

Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, ul. Narutowicza 11/12, 80-952 Gdansk-Wrzeszcz, Poland

Available online 17 January 2007

Abstract

The IEEE 802.11 MAC protocol now prevailing in wireless LANs is vulnerable to selfish *backoff attacks* consisting in selection of short backoff times in the constituent CSMA/CA procedure. Administrative prevention of such attacks fails in ad hoc configurations, where stations' behavior cannot be mandated. In this paper we take an incentive-oriented game-theoretic approach whereby stations are allowed to maximize their payoffs (achieved success rates). Using a fairly accurate performance model we show that a noncooperative CSMA/CA game then arises with a payoff structure characteristic of a Prisoners' Dilemma. For a repeated CSMA/CA game, a novel SPELL strategy is proposed and shown to yield to simple algorithmic design. Assuming that the stations are rational players and wish to maximize a mean-value-type long-term utility, SPELL is further shown to deter a single attacker by providing a disincentive to deviate from SPELL.
© 2006 Elsevier B.V. All rights reserved.

Keywords: Wireless LAN; CSMA/CA; Game theory

1. Introduction

The prevailing MAC protocol for ad hoc wireless local-area networks (LANs) is IEEE 802.11 DCF [10] (see Table 1 for an explanation of related acronyms). Its key mechanism called CSMA/CA has a transmitting station back off for a random time upon a frame collision to avoid further collisions. While utilizing the channel bandwidth efficiently provided that all the stations are cooperative, CSMA/CA may potentially foster selfish behavior consisting in systematic selection of incorrectly short backoff times, further called a *backoff attack*. Evidence from simulation and experimentation [3,18] shows that a backoff attack brings about long-term unfairness (an unfairly large long-term bandwidth share for an attacking station at the cost of the other LAN stations) on top of the well-known phenomenon of IEEE 802.11 short-term unfairness [12]. Nowadays such an attack is also easy to launch with user-accessible software [3] and hence becomes a major security concern for honest users.

Existing approaches to backoff attacks rely on identification of the culprits via anomaly detection algorithms and subsequent selective penalization using administrative leverage or reputation schemes [14,18], random jamming [5,17], or forced randomness of backoff times (thus entailing a major overhaul of IEEE 802.11) [6]. Behind all these approaches is the need for an authentication infrastructure, which ad hoc networks typically lack. This paper addresses the problem in a game-theoretic framework and offers some algorithmic disincentives to potential attackers, while not

* Tel.: +48 58 347 2123.
E-mail address: jekon@eti.pg.gda.pl.

1570-8667/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jda.2006.12.004

Table 1
IEEE 802.11-related acronyms

CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DSSS	direct sequence spread spectrum
FHSS	frequency hopping spread spectrum
IEEE	Institute of Electrical and Electronics Engineers
MAC	medium access control
NAV	Network Allocation Vector
OFDM	orthogonal frequency division multiplexing
RTS	Request to Send
SIFS	Short Interframe Space

affecting CSMA/CA operation and permitting station anonymity. We thus contribute to the still underexplored area of game-theoretic design of distributed MAC protocols resilient to selfish behavior (cf. [1,2,5,13,15,17,21,23]). At the core of the proposed solution is the recognition, based on the observed network performance, of the number of stations currently launching a backoff attack; for this purpose, a fairly accurate model of CSMA/CA performance under backoff attack is presented. Next we propose a station strategy called SPELL that permits to reach a *subgame perfect Nash equilibrium* (NE). Informally, if all the stations use SPELL then ultimately all of them play honestly, whereas a station deviating from SPELL by persistently attempting a backoff attack is asymptotically punished; however, if it reverts to SPELL at any time then the punishment ultimately becomes imperceptible.

In Section 2 we describe a wireless LAN model and discuss related work. Stochastic performance under a backoff attack is studied in Section 3. In Section 4 we define one-shot and repeated CSMA/CA games. SPELL is described and analyzed in Section 5. Section 6 concludes and outlines further research.

2. Backoff attack scenery

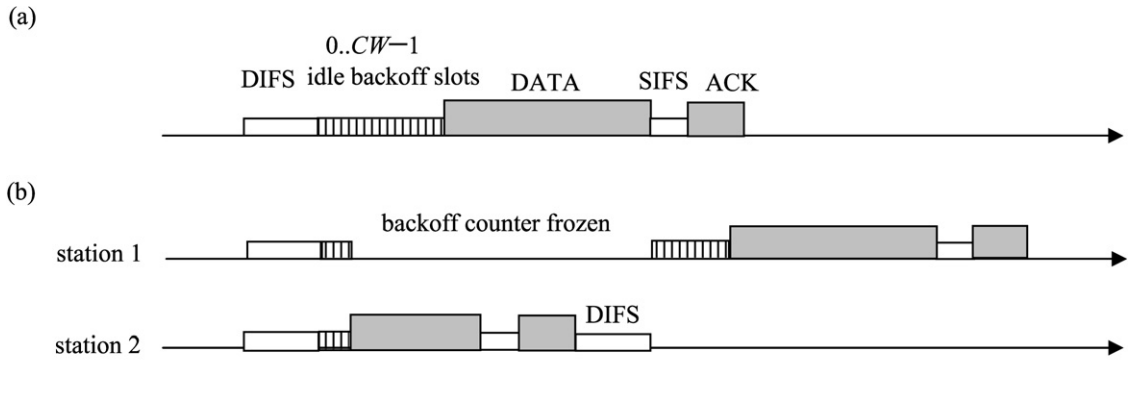
Below we state the network model, briefly summarize CSMA/CA operation, and look at some related work on selfish MAC-layer behavior.

2.1. Network operation

Consider a full-coverage ad hoc wireless LAN with N stations using the IEEE 802.11 MAC-layer protocol [10] to access a single channel. We assume negligible inter-station propagation delays and perfect channel and station operation. Furthermore we assume that: (1) the network operates under saturation i.e., each station is always ready to transmit user packets in the form of DATA frames, and (2) a station remains anonymous to non-recipients in that, based on a set of frames sensed on the medium, no non-recipient can either (a) deduce the identity of the sender or recipients, or even (b) reliably detect that any two frames have a common sender or recipient.

Assumption 1 motivates selfish behavior: it is only under heavy load that the stations get interested in achieving larger-than-fair bandwidth shares. Part (a) of assumption 2 rules out selective punishment for a backoff attack, whereas part (b) renders backoff attacks undetectable by means of statistical traffic analysis. This assumption is justified by the fact that a station's physical identity (location) is untraceable due to mobility and the lack of tracking devices within the network, whereas its logical identity (e.g., network-layer address) can be obscured by fictitious MAC addresses (with any true identity information possibly encrypted end-to-end in the DATA frame payload). It seems reasonable to design countermeasures against backoff attacks under assumption 2, as they then provide a "security lower bound" for countermeasures relying on station identification.

CSMA/CA operates as follows. If the *basic access* method is used then, upon a DATA frame transmission, a station waits until the medium has been sensed idle for a predefined DIFS interval. Then it sets a local *backoff counter* to a random value between 0 and $CW - 1$, where CW is the current *contention window*. Initially, CW is set to a minimum $w_{\min}$. The backoff counter is decremented each time the medium is sensed idle for a predefined *slot* interval, with the countdown frozen whenever the medium is sensed busy and resumed after it is sensed idle for another DIFS interval.



(c)

1) transmit DATA / RTS frame;
2) **if** ACK / CTS received **then** $CW := w_{\min}$ **else** $CW := \min\{2 \cdot CW, w_{\max}\}$
3) backoff counter := random $[0, CW - 1]$;
4) wait **until** medium sensed idle for DIFS interval;
5) **while** (backoff counter > 0) **and** (medium sensed idle) **do**
   decrement backoff counter in each slot;
6) **if** medium sensed busy **then** go to 4) **else** go to 1)

Fig. 1. CSMA/CA operation; (a) DATA + ACK exchange, (b) backoff freezing, (c) simplified pseudocode.

When the backoff counter has reached zero the station understands it has captured a "virtual token" and transmits a DATA frame. If successful, the frame is responded to by a recipient's ACK frame and CW is reset to $w_{\min}$. Otherwise i.e., if several stations simultaneously capture the "virtual token", their DATA frames collide, but each of them will have inferred a collision from the lack of ACK response. Subsequently it will double CW (unless a maximum $w_{\max}$ has been reached), set the backoff counter to a random integer from the range $[0, CW - 1]$, and start another countdown. Consecutive collisions beyond a certain limit cause a transmission abort; we neglect this feature in our model. A SIFS interval, shorter than DIFS, is specified to guarantee uninterrupted DATA + ACK exchange.

If the *RTS/CTS access* method is used, a station whose backoff counter has reached zero transmits a short RTS frame. A successful RTS frame is responded to by a recipient's short CTS frame and a DATA frame transmission follows. If two or more stations simultaneously transmit RTS frames, they will infer a collision (since no CTS frame follows), double their contention windows and set their backoff counters similarly as before. A SIFS interval guarantees uninterrupted four-way exchange of successful RTS and then CTS, DATA, and ACK frames. Fig. 1 illustrates the workings of CSMA/CA under basic access IEEE 802.11 DCF in a simplified way; the timing of a DATA + ACK exchange without interference of other stations is shown in Fig. 1(a), whereas in Fig. 1(b), station 1 is beaten by station 2 to a DATA frame transmission and freezes its backoff counter until another DIFS period of idle medium is detected. Fig. 1(c) presents a simplified pseudocode of CSMA/CA operation under IEEE 802.11 DCF.

We complete the model by assuming that (3) at each station, the local $w_{\min}$ and $w_{\max}$ are configurable by user accessible software. Assumption 3 enables a backoff attack; see [18] and vendor data for details of manipulating these parameters in some existing network adapters. We rule out, however, selfish or malicious tampering with any other IEEE 802.11 parameters or functions e.g., DIFS or NAV; such tampering can be prevented or detected using simple means [3].

2.2. Related work

Existing approaches to backoff attacks (more generally, to MAC-layer selfish behavior) can be categorized as detection and penalization-based, and incentive-based (game-theoretic). The first approach relies on identification of the culprits via statistical anomaly detection, and subsequent selective penalization using reputation; these schemes require as prerequisites a distributed authentication infrastructure, hard to come by in ad hoc systems, a reputation infrastructure with its communication and processing overhead, as well as stations' willingness to build reputation

rather than just capturing a large bandwidth share. The second approach defines game payoffs such that rational behavior at each station (playing the game to maximize payoff) leads to a globally acceptable outcome e.g., high total bandwidth utilization. Although the literature following the two approaches appears to form separate lines of research, the distinction between them is in fact not sharp: the prospect of a penalty can be viewed as a cost constituent of game payoffs and a disincentive to launch a backoff attack. From a different angle, the presence of a dedicated subsystem supporting penalties e.g., reputation database, qualifies as the first approach. Game-theoretic papers can be further categorized depending on the (subjectively assessed) level of exogeneity of the game payoffs: "purely" game-theoretic solutions only account for the endogenous (self-imposed) figures of merit i.e., the received bandwidth shares; second-tier solutions introduce combined payoffs such as the ratio, or linear combination, of the bandwidth shares and power consumption, believed to be self-imposed by the players (hence, containing the researcher's beliefs as an exogenous element); third-tier solutions include completely exogenous payoff constituents such as reputation.

Within the detection and penalization-based approach, concrete solutions differ primarily in the means of detection of a backoff attack they attempt to create. In [14], a recipient controlled backoff scheme is proposed whereby successive backoff times are announced by the recipients of the intended DATA frame transmissions, rather than being drawn from the range $[0, CW-1]$ at a sender station (this implies a major overhaul of IEEE 802.11). A sender's disobedience is detected at the recipient by comparing the observed and announced number of empty slots preceding a given DATA frame, and punished by announcing a larger backoff for the next frame from that sender. Neither of these two steps is trivial: the former has to cope with interleaved transmission from several sender stations and with CW expansion upon collisions, not all of which are perceptible to the recipient assuming there may be hidden stations; the latter must ensure fairness among all the senders transmitting to one recipient and the punishment must be administered with restraint in view of possible false detections of disobedience. Persistent disobedience is diagnosed and reported to a reputation system. Apart from violation of the MAC standard, the solution may be criticized for the need of a costly authentication and reputation infrastructure. Moreover, it only works assuming the recipient never misbehaves or colludes with any of its senders (the latter is particularly rash given that a sender and recipient are tied by a common interest). In [6], simple cryptography is used to produce an improvement ensuring randomness of each backoff time—i.e., the sender can be certain it is not being punished without a reason, while being unable to launch an undetected backoff attack. The RTS + CTS + DATA + ACK exchange is a vehicle for a coin flipping scheme: the recipient commits to a random value R by announcing its hash $\tilde{R}$ in the CTS frame; subsequently the sender appends another random value S to the DATA frame and finally the recipient announces R in the ACK frame, whereupon the next backoff time is computed as the bit-by-bit exclusive-OR of R and S. If the sender detects that the hash of R does not match $\tilde{R}$ it can report the recipient as misbehaving. The scheme in itself does not address sender-recipient collusion, which is left to a third party using complex statistical anomaly detection algorithms. Moreover, extra transmission overhead is imposed to transport $\tilde{R}$, S, and R. Finally, like in the previous solution, an authentication infrastructure is necessary.

Another solution also within the above approach [18] leaves the MAC standard intact, but besides station authentication requires the presence of a trusted party known to never misbehave (therefore is mainly suitable for hot-spot wireless LANs). The trusted party (usually the access point) is equipped with a software agent called DOMINO, responsible for backoff attack detection and penalization; to detect deviations from supposedly random backoff times at each station, a number of statistical tests are employed based on observation of separation times between consecutive DATA frames. (Some of the tests have been criticized and improved in [6].)

A simple game-theoretic solution is presented in [17]. Each station's strategic options are confined to "timid" (observing IEEE 802.11 DCF), "greedy" (backoff counter disengaged), and "player". The latter option drives the stations away from playing "greedy" by selective jamming of their DATA frames; a "greedy" station is recognized as such upon receipt of a predefined number of consecutive DATA frames from that station (thus authentication is again necessary). Although the reasoning is purely intuitive and lacks game-theoretic analysis, the basic conjecture—that a "player" station should administer jamming so as to equalize "greedy" and "player" bandwidth shares—is close to postulating the convergence to a Nash equilibrium (NE) different from "all-greedy". A more systematic study in the same spirit is presented in [5]. Game payoffs are defined as weighted combinations of received bandwidth shares and excess transmission rates over some target value. From the Kuhn–Tucker theorem the authors derive the existence and uniqueness of a NE, whose location can be controlled by appropriate choice of the weights, in particular can be close to Pareto optimality. Next a dynamic game is described where each station adjusts its transmission rate in proportion to the payoff derivative with respect to the transmission rate, which, by Lyapunov's stability theorem, guarantees

reaching the NE. Related implementation challenges are serious: a common target transmission rate has to be agreed on; to enforce the target each station must measure its own bandwidth share and compare with the other stations' (which again requires station authentication); upon a series of adjustments leading to a temporary stabilization of the transmission rates, a station with a currently smaller transmission rate must penalize those with currently larger transmission rates by jamming their DATA frames, a violation of the MAC standard. To avoid driving the target rate to zero, jamming is not allowed until the adjustments are over, a provision hard to enforce. Note that the above game-theoretic solutions are "pure" in that they only introduce endogenous payoffs (namely, the stations' bandwidth shares).

Constrained optimization in a game-theoretic context is also used in [7]. The authors focus on the rarely addressed issue of selfish MAC-layer behavior in multihop IEEE 802.11 mobile ad hoc networks. In a conceptual link contention graph, vertices are station-to-station wireless links (two stations being within each other's transmission range) and vertex adjacency reflects the sender or recipient of one link being within the interference range of the sender or recipient of the other. Any maximal clique in such a graph (a fully connected subgraph not being a subgraph of another fully connected subgraph) represents a collision domain (a set of links that can be used by one DATA frame at a time). Network optimization then consists in maximizing a sum of end-to-end flow satisfaction measures subject to the capacity constraints associated with each maximal clique. This can be turned via Lagrangian relaxation into a dynamic noncooperative game, each flow being assigned a combined satisfaction and capacity-related payoff to be maximized individually by a series of gradient search-type adjustments of *CW* at the stations it traverses. The game ends up at a unique NE whose location, because of the capacity constraints, is away from "all-greedy". In a proposed implementation, *CW* adjustments use feedback from the network, with increased collision rates and queuing delays indicating that a clique capacity is being approached. It might appear that this solution is not "purely" game-theoretic since clique capacity constraints are exogenous—one could doubt why a station sending a flow down the next link along an end-to-end path should be concerned about flows on other links. However, some other links of a clique may be used by the flow further down the path and so reflect upon the flow's satisfaction. The solution is also interesting as it does not require station authentication. Unfortunately, it is not applicable to ad hoc LANs, where the maximal clique covers all of the network and no capacity constraint keeps the NE away from "all-greedy" (i.e., there is a uniform incentive to launch a backoff attack).

3. Stochastic performance model

We analyze saturated CSMA/CA under backoff attack using a station's success rate as a performance measure; thereby we factor out DATA and control frame lengths, MAC- and physical-layer timing parameters, as well as the access method (basic or RTS/CTS).

3.1. Performance of saturated CSMA/CA

Define L so that $w_{\max} = w_{\min} \cdot 2^L$, thus the backoff scheme is fully characterized by a pair $w = \langle w_{\min}, L\rangle$ (e.g., $w = \langle 16, 6\rangle$ is recommended for 54 Mb/s OFDM-based or 1 Mb/s FHSS-based physical layer, and $w = \langle 32, 5\rangle$ is recommended for 11 Mb/s DSSS-based physical layer).

Bianchi [4] introduces a Markovian model of CSMA/CA under saturation, assuming a common configuration $\langle w_{\min}, L\rangle$ at all stations and neglecting backoff freezing. His approach relies on an "independence hypothesis" whereby each station perceives the presence of the other stations through a constant probability c of a foreign transmission in any slot during backoff countdown. At each station, c can be interpreted as the rate of RTS or DATA frame transmission attempts by other stations, or as the inferred collision rate (percentage of own unsuccessful frame transmission attempts). Given c, the steady-state frame transmission rate at a station is shown to be $t(c) = 1/(\frac{w_{\min}+1}{2} + \frac{w_{\min}}{4} \cdot \sum_{l=1}^{L}(2c)^l)$. To reflect backoff freezing upon sensing the medium busy one can also write $t(c) = 1/B$, where B is the average value of the backoff counter upon a frame transmission.[1] The backoff counter is decremented in each slot where the medium is sensed idle; when it reaches zero, another attempt follows. On average, the backoff counter is frozen at any positive value for $1/(1-c)$ consecutive slots. Hence, $t(c) = 1/(\frac{B-1}{1-c} + 1) = \frac{1-c}{B-c}$,

[1] This is a consequence of the renewal-reward theorem; for further refinements of the model see e.g., [25].

or

$$t(c) = \frac{1-c}{(w_{\min}+1)/2 + (w_{\min}/4)\cdot\sum_{l=1}^{L}(2c)^l - c}. \tag{1}$$

By the "independence hypothesis", c can be determined as the unique solution of

$$c = 1 - \big[1 - t(c)\big]^{N-1}. \tag{2}$$

The solution of (2) and the corresponding transmission rate, $\hat{c}$ and $\hat{t}$, determine each station's achieved bandwidth share [4], which is, however, physical layer, access method, and DATA frame length specific. To remove dependence on these facets and focus on general properties of saturated CSMA/CA, we measure a station's performance as its *success rate*:

$$b = \frac{\hat{t}\cdot(1-\hat{c})}{\hat{T}}, \tag{3}$$

where $\hat{T} = 1-(1-\hat{t})^N$ is the total frame transmission rate. Thus b represents the rate of successful frame transmissions per busy backoff slot. Clearly, b is indicative of the achieved bandwidth share.[2]

3.2. Extension of Bianchi's model

Assume now that each station n can configure its backoff scheme individually with $w_n = \langle w_{n,\min}, L_n\rangle$ possibly departing from the IEEE 802.11 standard. Smaller $w_{n,\min}$ and L_n correspond to a "more selfish" station n i.e., the more it deprives the other ones of transmission opportunity. In fact, unless $w_n = \langle 1, L\rangle$ is allowed, the most selfish backoff configuration is $w_n = \langle 2, 0\rangle$, whereby station n backs off for one slot only, or does not back off at all regardless of inferred collisions. Any "less selfish" configuration could lead to station n being outperformed by stations adopting $\langle 2, 0\rangle$. $w_n = \langle 1, L\rangle$ could be impractical, as it would cut off all the other stations, including those with which station n might wish to communicate. We discuss $w_n = \langle 1, 0\rangle$ in Section 5.3.

To focus on realistic scenarios, we do not explore the possibility of a different backoff scheme configuration at each station; instead we assume that x stations out of N adopt a self-optimized backoff scheme configuration, while the other $N-x$ adopt the standard configuration prescribed for the present physical layer. Thus x stations are *selfish* with $w_n = w_{\mathrm{s}} = \langle 2, 0\rangle$, and $N-x$ stations are *honest* with $w_n = w_{\mathrm{h}}$, where w_{h} is significantly "larger" than w_{s} (e.g., $w_{\mathrm{h}} = \langle 16, 6\rangle$ or $\langle 32, 5\rangle$). Note that the inferred collision rates may differ at honest and selfish stations, so we write c_{h} and c_{s}. It is natural to extend Bianchi's model to get expressions for $t_{\mathrm{h}}(c_{\mathrm{h}})$ and $t_{\mathrm{s}}(c_{\mathrm{s}})$ similar to (1). This leads to a fixed-point relationship in c_{h} and c_{s} analogous to (2):

$$\begin{aligned} c_{\mathrm{h}} &= 1 - \big[1 - t_{\mathrm{h}}(c_{\mathrm{h}})\big]^{N-x-1}\big[1 - t_{\mathrm{s}}(c_{\mathrm{s}})\big]^{x},\\ c_{\mathrm{s}} &= 1 - \big[1 - t_{\mathrm{s}}(c_{\mathrm{s}})\big]^{x-1}\big[1 - t_{\mathrm{h}}(c_{\mathrm{h}})\big]^{N-x}, \quad x = 1,\ldots,N-1 \end{aligned} \tag{4}$$

(the cases $x = 0$ and $x = N$ reduce to (2)). Numerical analysis shows that for $w_{\mathrm{s}} = \langle 2, 0\rangle$ and any w_{h} prescribed for various existing physical layer technologies, (4) admits a unique solution $(\hat{c}_{\mathrm{h}}, \hat{c}_{\mathrm{s}})$; let $(\hat{t}_{\mathrm{h}}, \hat{t}_{\mathrm{s}})$ be the corresponding frame transmission rates. The success rates of a selfish and honest station are respectively $b_{\mathrm{h}} = \hat{t}_{\mathrm{h}}\cdot(1-\hat{c}_{\mathrm{h}})/\hat{T}$ and $b_{\mathrm{s}} = \hat{t}_{\mathrm{s}}\cdot(1-\hat{c}_{\mathrm{s}})/\hat{T}$, where $\hat{T} = 1-(1-\hat{t}_{\mathrm{s}})^x(1-\hat{t}_{\mathrm{h}})^{N-x}$.

3.3. Mixed model

Since it hinges upon the "independence hypothesis", the above extension of Bianchi's model becomes less accurate, the more frequent and correlated are frame collisions. Given that selfish stations tend to configure $w_{\min}$ and L much smaller than the standard recommends, such an extension can be expected to yield highly inaccurate frame transmission and collision rates at selfish stations, particularly if they are few. Assuming $w_{\mathrm{s}} = \langle 2, 0\rangle$, a *mixed model* described

[2] Although for extremely large contention windows the success rate grows to 100% as the bandwidth share approaches zero (since most of the bandwidth remains unused while all the stations' backoff counters drop from large values), we confine ourselves to realistic settings where the bandwidth share increases monotonously in the success rate.

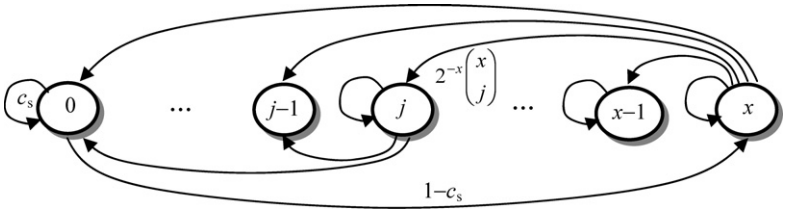


Fig. 2. State transitions for the "selfish aggregate".

below better captures the dynamics of CSMA/CA under saturation, as it alleviates the "independence hypothesis" within the set of selfish stations.

The mixed model comprises $N - x$ honest stations and one "selfish aggregate" representing all x selfish stations. The latter is modeled by a one-dimensional Markov chain with state space $\{0, \ldots, x\}$ depicted in Fig. 2. Each state encodes the number of selfish stations with expired backoff counters, hence attempting to transmit an RTS or DATA frame in the present slot. For legibility, only transitions from generic and boundary states are shown. From state $k > 0$, states $j = 0, \ldots, k$ can be directly reached; each such transition corresponds to exactly j out of k previously transmitting stations setting the backoff counter to zero for an immediate retransmission attempt. The self-loop at state 0 reflects all selfish stations freezing their backoff counters at one as they sense a frame transmission attempt by some honest stations; this happens with probability c_s, now interpreted as the total rate of frame transmission attempts by all the honest stations. Finally, the transition from state 0 to state x occurs when all the selfish stations decrement their backoff counters upon sensing the medium idle. Instead of finding the steady-state probabilities we note that for the selfish stations,

$$t_s(c_s) = \frac{\Gamma_x}{\Gamma_x + c_s/(1-c_s) + 1}, \tag{5}$$

$$b_s = \frac{2 \cdot \Psi_x \cdot (1-c_s)}{x \cdot [\Gamma_x + c_s/(1-c_s)]}, \tag{6}$$

where Γ_x is the first-passage time from state x to state 0 and Ψ_x is the probability that the passage does not omit state 1. To explain (5), divide the operation of the "selfish aggregate" into cycles. Each cycle starts at state x and until state 0 is reached (after Γ_x slots on average), each subsequent slot contains a frame transmission attempt by a selfish station. Then the honest stations attempt their frame transmissions; by the "independence assumption", this occurs in $c_s/(1-c_s)$ consecutive slots on average and is followed by an idle slot, whereupon the selfish stations' backoff counters are decremented to reach zero and the cycle begins anew. Thus $c_s/(1-c_s)+1$ represents the average sojourn time in state 0, where none of the selfish stations transmit. In (6), the factor $2 = 1/(1-1/2)$ in the numerator is the average sojourn time in state 1 (consecutive frame transmission attempts by a single selfish station followed by setting the backoff counter to zero). Thus the numerator represents the average number of successful frame transmission attempts by a selfish station per cycle, whereas $\Gamma_x + c_s/(1-c_s)$ is the average number of busy slots per cycle. The division by x reflects a fair distribution of the "selfish aggregate" success rate among the selfish stations.

The following recurrence relationships can be deduced from Fig. 2:

$$\Gamma_x = 1 + 2^{-x} \sum_{j=0}^{x} \binom{x}{j} \Gamma_j, \quad x \geqslant 1 \tag{7}$$

$$\Psi_x = 2^{-x} \sum_{j=0}^{x} \binom{x}{j} \Psi_j, \quad x \geqslant 2 \tag{8}$$

with $\Gamma_0 = 0$, $\Psi_0 = 0$, and $\Psi_1 = 1$. Recurrences of this type arise in the analysis of incomplete digital trees and can be solved using exponential generating functions [19] or Poisson generating functions [20]. Recall that for an infinite sequence of real numbers $(a_x)_{x=0,1,2,\ldots}$, the Poisson generating function is defined as $H_a(z) = \sum_{x=0}^{\infty} e^{-z} \frac{z^x}{x!} a_x$. Given $H_a(z)$ and its power series expansion $\sum_{j=0}^{\infty} \frac{h_j}{j!} z^j$, one can recover the original sequence as $a_x = \sum_{j=0}^{x} \binom{x}{j} h_j$. Another property that comes in handy when analyzing (7) and (8) is that the Poisson generating function of the sequence $(2^{-x} \sum_{j=0}^{x} \binom{x}{j} a_j)_{x=0,1,2,\ldots}$ is $H_a(z/2)$. Applying these two properties, multiplying both sides of (7) by

$e^{-z}\frac{z^x}{x!}$, summing over $x = 0, 1, 2, \ldots$, and taking into account the initial condition $\Gamma_0 = 0$, we get the functional equation:

$$H_\Gamma(z) = \sum_{x=1}^{\infty} \frac{e^{-z} \cdot z^x}{x!} + H_\Gamma(z/2) - \Gamma_0$$

i.e., $H_\Gamma(z) - H_\Gamma(z/2) = 1 - e^{-z}$. Expanding both sides into power series and comparing the coefficients at equal powers of z we arrive at $h_0 = 0$ and $h_j = \frac{(-1)^{j+1}}{(1-2^{-j})}$ for $j > 0$, and finally

$$\Gamma_x = \sum_{j=0}^{x} \binom{x}{j} \frac{(-1)^{j+1}}{1 - 2^{-j}}. \tag{9}$$

Applying a Poisson generating function to (8), taking into account the initial conditions $\Psi_0 = 0$ and $\Psi_1 = 1$, and calculating along the same lines as for the Γ_x leads to the functional equation:

$$H_\Psi(z) = e^{-z} \cdot z + H_\Psi(z/2) - \Psi_0 - \frac{\Psi_1}{2} \cdot e^{-z} \cdot z$$

i.e., $H_\Psi(z) - H_\Psi(z/2) = z \cdot e^{-z}/2$. Hence, $h_0 = 0$ and $h_j = \frac{j(-1)^{j-1}}{2(1-2^{-j})}$ for $j > 0$, and finally

$$\Psi_x = x \cdot \sum_{j=0}^{x-1} \binom{x-1}{j} \frac{(-1)^j}{2 - 2^{-j}}. \tag{10}$$

The success rates of honest stations are obtained similarly as in Section 3.2 using (1) and solving

$$\begin{aligned} c_h &= 1 - \big[1 - t_h(c_h)\big]^{N-x-1}\big[1 - t_s(c_s)\big], \\ c_s &= 1 - \big[1 - t_h(c_h)\big]^{N-x}, \quad x = 1, \ldots, N-1 \end{aligned} \tag{11}$$

(the cases $x = 0$ and $x = N$ reduce to (2)). Like (4), (11) can be shown via numerical calculation to admit a unique solution for existing physical layer technologies.

In further presentation we indicate the dependence of the stations' success rates on N and x. Table 2 presents $b_h(N, x)$, $b_s(N, x)$, and the total success rate $b_\Sigma(N, x) = (N - x) \cdot b_h(N, x) + x \cdot b_s(N, x)$ obtained from the mixed model for $N = 10$ and 20, assuming $w_h = \langle 16, 6\rangle$. The results were validated using Monte Carlo simulation, with 95% confidence intervals reduced to less than 1% of the obtained sample averages. For comparison, analysis using extended Bianchi model was also carried out. Table 2 also contains relative errors of $b_s(N, x)$ produced by both models with respect to simulation (italicized entries; left: mixed model, right: extended Bianchi model). Note that while the mixed model yields a good match with simulation, it slightly underestimates $b_s(N, x)$; still, the approximation is far better than that of the extended Bianchi model.

Table 2 illustrates that for any N and $x < N$, $b_s(N, x + 1)$ and $b_h(N, x)$ decrease in x and

$$b_s(N, x + 1) > b_h(N, x), \tag{12}$$

Table 2
Success rates obtained from the mixed model

x	$b_h(N,x)$, $b_s(N,x)$(%), and relative error of $b_s(N,x)$(%)								$b_\Sigma(N,x)$(%)	
	$N = 10$				$N = 20$				$N = 10$	$N = 20$
0	8.1		mixed	EBM	3.8		mixed	EBM		
1	0.2	94.7	*−4.4*	*−5.8*	0.2	89.6	*−8.7*	*−11.7*	96.5	93.1
2	0.1	24.4	*−2.5*	*29.5*	0.1	23.6	*−5.5*	*24.8*	49.4	48.8
3	0.1	14.9	*−1.4*	*16.2*	0.1	14.6	*−3.8*	*12.7*	45.1	44.7
4	0	10.2	*−0.9*	*10.8*	0	10.0	*−2.8*	*7.0*	41.1	40.8
5	0	7.6	*−0.7*	*7.0*	0	7.5	*−2.7*	*2.9*	38.0	37.7
10		3.1	*0.1*	*−4.3*	0	3.0	*−1.2*	*−9.2*	30.5	30.4
20						1.3	*0.3*	*−20.7*		25.4

$$b_s(N, N) < b_h(N, 0). \tag{13}$$

That is, a station always benefits by playing selfishly, yet too many selfish stations become worse off than they would be if all of them were playing honestly. The critical number of selfish stations at which that happens is close to $N/2$ e.g., equals 3, 5, 7, and 9 respectively for $N = 5, 10, 15$, and 20. Before we consider the above results from a game-theoretic angle, let us point to three more features invariant across a wide range of N.[3] First, $b_h(N, 0)$ is distinctly nonzero, while $b_h(N, x) \approx 0$ for $x > 0$; second, $b_s(N, x)$ distinctly drops with x if x is not too large; finally, $b_\Sigma(N, x)$ varies much less distinctly with N than with x. Using these and by observing its own and the total success rate, each station n can infer x with a certain granularity (even though it has no means of knowing N or w_m for $m \neq n$, and the success rates may be observed inaccurately). If $w_n = w_s$, observation of b_n permits to distinguish the cases $x = 1, \ldots, x = x^*$, and $x > x^*$, where $x^* \leqslant 5$. If $w_n = w_h$, a similar distinction follows from the observed b_Σ, while observation of b_n yields a distinction between $x = 0$ and $x > 0$. (Even in our anonymous setting, b_Σ is observable via monitoring of successful DATA + ACK exchanges.)

4. CSMA/CA game

Given the choice between w_h and w_s, each station pursues a maximum success rate independently of (i.e., not seeking binding agreements with) the other stations; yet the result depends not only on its own choice, but also the other stations'. Thus a noncooperative N-player *CSMA/CA game* arises, in which success rates are the payoffs. Below we recall a few basic notions of game theory [9] in the context of our network model. First we consider a one-shot game, in which selection of w_h or w_s is a single act performed simultaneously at all the stations.

Definition 1. A CSMA/CA game is a triple $(\{1, \ldots, N\}, W, b)$, where $\{1, \ldots, N\}$ is the set of players (stations), $W = \{w_h, w_s\}$ is the set of feasible actions (backoff scheme configurations), and $b : W^N \to \mathbf{R}^N$ is a payoff function. Each station n selects $w_n \in W$ and subsequently receives a payoff (success rate) $b_n(\boldsymbol{w})$ dependent on the action profile $\boldsymbol{w} = (w_n, \boldsymbol{w}_{-n})$, where $\boldsymbol{w}_{-n}$ represents the opponent profile i.e., the actions selected by all the stations besides n.

Definition 2. An action w is a *best reply* to $\boldsymbol{w}_{-n}$ if $b_n(w, \boldsymbol{w}_{-n}) \geqslant b_n(w', \boldsymbol{w}_{-n})$ for all $w' \in W$. Let $BR(\boldsymbol{w}_{-n})$ denote the set of best replies to $\boldsymbol{w}_{-n}$. A *Nash equilibrium* (NE) is an action profile $\boldsymbol{w} = (w_n, \boldsymbol{w}_{-n})$ at which $w_n \in BR(\boldsymbol{w}_{-n})$ for all $n = 1, \ldots, N$.

That is, a NE is an action profile where each station has selected a best reply to the opponent profile, hence one from which no station has an incentive to deviate unilaterally. Such an outcome can be expected when all the stations are rational (i.e., only interested in maximizing their own payoffs) and their rationality is common knowledge [9].

Definition 3. An action profile $\boldsymbol{w} \in W^N$ is *fair* if $b_1(\boldsymbol{w}) = \cdots = b_N(\boldsymbol{w})$. A fair action profile $\boldsymbol{w}$ is *efficient* if $b_n(\boldsymbol{w}) \geqslant b_n(\boldsymbol{w'})$ for any other fair action profile $\boldsymbol{w'}$.

In the CSMA/CA game, $b_n(w_n, \boldsymbol{w}_{-n}) = b_h(N, x)$ if $w_n = w_h$ and $b_n(w_n, \boldsymbol{w}_{-n}) = b_s(N, x)$ if $w_n = w_s$, where x is the cardinality of the set $\{n = 1, \ldots, N \mid w_n = w_s\}$. As Table 2 shows, the only fair action profiles are all-w_h and all-w_s (all stations selecting w_h and w_s, respectively), of which only the former is efficient, cf. (13). Thus all-w_h is a desirable outcome from the global design viewpoint, as it corresponds to a cooperative ("live-and-let-live") scenario. Unfortunately, it is not a NE: as seen from (12), $BR(\boldsymbol{w}_{-n}) = \{w_s\}$ for any n and any $\boldsymbol{w}_{-n}$, implying that the unique (and inefficient) NE is all-w_s. It follows that the CSMA/CA game is a multiplayer *Prisoners' Dilemma* [24], where playing selfish is a *dominating action* (the best reply to any opponent profile, as determined by (12)) and the payoffs of all players decrease with the number of selfish players; the latter feature implies that the dominating actions intersect at an inefficient NE (as determined by (13)).

We now wish to model a situation where the stations may learn from past experience and, in pursuit of a longer-term goal, may incline to honest play in search for efficient action profiles. A suitable framework is that of repeated

[3] For $N \leqslant 20$, $b_h(N, 0) \geqslant 3\%$, while $b_h(N, x) < 1\%$ for $x > 0$; moreover, if $x \leqslant 5$ then $b_h(N, x + 1)$ is at least 20% less than $b_h(N, x)$, and for any $N, N' \leqslant 20$, $b_\Sigma(N, x + 1)$ is at least 6% less than $b_\Sigma(N', x)$. Note that 20 seems a reasonable upper bound for the number of wireless LAN stations simultaneously operating at saturation.

games [9]. Consider a *repeated CSMA/CA game* consisting of multiple stages, each of which is an instance of one-shot CSMA/CA game. For each stage $k = 1, 2, \ldots$, station n selects $w_n^k \in \{w_\mathrm{s}, w_\mathrm{h}\}$ so that $\boldsymbol{w}^k = (w_1^k, \ldots, w_N^k)$ is the resulting action profile, whereas the received stage payoffs are

$$b_n^k = \begin{cases} b_\mathrm{s}(N, x^k), & \text{if } w_n^k = w_\mathrm{s}, \\ b_\mathrm{h}(N, x^k), & \text{if } w_n^k = w_\mathrm{h}, \end{cases} \tag{14}$$

with $x^k = |\{m = 1, \ldots, N \mid w_m^k = w_\mathrm{s}\}|$. $(x^1, \ldots, x^k)$ is the *play path* up to stage k; in view of our earlier discussion, it is common knowledge to all the stations. Given the current play path, station n's *strategy* σ_n specifies the probability of selecting $w_n^{k+1} = w_\mathrm{s}$ i.e., $\sigma_n : \Pi \to [0, 1]$, where Π is the set of all finite-length play paths. Along with the strategy profile $\boldsymbol{\sigma} = (\sigma_n, \boldsymbol{\sigma}_{-n})$, a play path $\boldsymbol{\pi} \in \Pi$ induces a probability distribution $\mu(\sigma_n \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi})$ of future b_n^k, and hence the future average stage payoffs $E_{\mu(\sigma_n, \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi})} b_n^k$. The long-term *utility* station n maximizes is a limit inferior-type asymptotic [11]:[4]

$$u_n(\sigma_n, \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi}) = \liminf_{k \to \infty} E_{\mu(\sigma_n, \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi})} b_n^k. \tag{15}$$

A desirable strategy σ^* satisfies

$$b_\mathrm{h}(N, 0) = u_n\big(\sigma^*, (\sigma^*, \ldots, \sigma^*); \boldsymbol{\pi}\big) \geqslant u_n\big(\sigma, (\sigma^*, \ldots, \sigma^*); \boldsymbol{\pi}\big) \tag{16}$$

for all $n = 1, \ldots, N$, and any strategy σ and play path $\boldsymbol{\pi} \in \Pi$. The equality in (16) implies that ultimately the "live-and-let-live" (all-w_h) scenario prevails, whereas the inequality states that the strategy profile all-σ^* is a *subgame perfect* NE [9].

5. SPELL strategy

In this section we present a strategy called *Selfish Play to Elicit "Live-and-let-Live"* (SPELL) that satisfies (16) on conditions specified below. A station deviating from SPELL cannot improve its utility if the others play SPELL. If, however, it does deviate and finds its payoffs worsening (perhaps after an initial improvement), it can revert to SPELL at any time, ending up in a "live-and-let-live" scenario.

5.1. Description

SPELL is configured with two integer parameters, Y and M, and a sequence $(\boldsymbol{P}^r)_{r=1,2,\ldots}$ of complementary probability distribution functions over positive integers. The play proceeds in *spells*, each lasting a random number of stages drawn from $\boldsymbol{P}^r$ i.e., Pr[spell lasts $\geqslant i$ stages] $= P^r(i)$. As r increases, $\boldsymbol{P}^r$ should favor longer spells (this is stated more precisely in Lemma 2 below). If a spell lasts at most Y stages then w_h is selected throughout; otherwise w_s is selected in all but the last Y stages (Fig. 3). A station playing SPELL maintains an r-counter and a q-counter. Occasionally, q is disengaged, whereupon the station selects w_h in each stage until q is engaged again; this is controlled by the x^k inferred from b_n^k and b_Σ^k as explained in Section 3. When engaged, q is set to a random number Q drawn from $\boldsymbol{P}^r$, decremented after each stage, and upon reaching zero again set to a random number Q drawn from $\boldsymbol{P}^r$, so that w_s is selected when $q > Y$ and w_h otherwise. Until the station quits the game (e.g., has nothing to transmit), r can only be incremented. At the start of the game SPELL initializes r and engages q, and subsequently cycles through the following steps:

1) play out successive spells using q and $\boldsymbol{P}^r$ until $x^k \leqslant M$, whereupon q is disengaged;

2) play honestly until $x^k > 0$, whereupon engage q and increment r.

Fig. 4(a) shows the corresponding per-stage state transition diagram and Fig. 4(b) illustrates the above description with a simple scenario for $N = 3$, where all the stations initially play SPELL with $M = 1$ and $Y = 2$ (point k on the horizontal axis marks the end of stage k). Prior to stage 1 the q-counters at stations 1, 2, and 3 read respectively 6, 5, and 3; accordingly, honest play starts in stages 5, 4, and 2. In stage 4, station 3 starts playing selfishly again since its q-counter has reached zero. This happens before either of the other stations starts playing honestly, thus the q-counters remain engaged. The first stage where at most M stations play selfishly is stage 5, whereupon the q-counters are

[4] $\liminf_{k \to \infty} a_k = \lim_{k \to \infty} \inf\{a_k, a_{k+1}, \ldots\}$ exists for any bounded sequence $(a_k)_{k=1,2,\ldots}$.

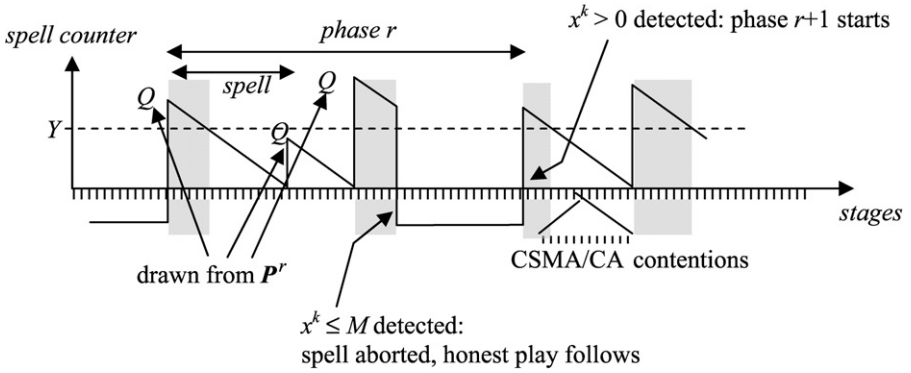


Fig. 3. q-counter operation (shaded areas indicate stages where w_s is selected).

disengaged and all-w_h persists until stage 9, where station 3 deviates by engaging its q-counter. In response, stations 1 and 2 engage their q-counters, increment their r-counters, and in the next stage start a new spell.

We make several remarks. First, if no station deviates from SPELL, step 2, once entered, is executed indefinitely producing a persistent all-w_h. Otherwise, the r-counter is incremented and ever longer spells are favored, thereby punishing a deviator who has to compete with more stations selecting w_s (recall from Section 3.3 that $b_\mathrm{s}(N, x)$ drops with x). Second, $0 < M \leqslant x^*$ should hold and only $x^k = 0, 1 \leqslant x^k \leqslant M$, and $x^k > M$ need to be distinguished. Finally, a stage should span enough CSMA/CA contentions to produce valid estimates of b_n^k and b_Σ^k.

5.2. Properties

We first look at sufficient conditions for SPELL to satisfy the left part of (16) if utility is defined by (15). More precisely, we want to establish that if all the stations play SPELL then the b_n^k converge in probability to $b_\mathrm{h}(N, 0)$ as k increases. The following two facts are useful:

Fact 1. [22] *Suppose a set of positive integers is closed under addition and has greatest common divisor one (i.e., the integers are relatively prime). Then there exists a threshold such that all consecutive integers above the threshold belong to the set.*

Fact 2. [8] *In a finite Markov chain containing transient and absorbing states, the number of state transitions to absorption is finite with probability one.*

Observe that at any station n playing SPELL, the current play path up to stage k only reflects upon the current values of the r-counter and q-counter, r_n^k and q_n^k; thus checking the left part of (16) for all play paths $\boldsymbol{\pi} \in \Pi$ amounts to checking for all possible current settings (r_n^k, q_n^k). Let $\mathrm{supp}(\boldsymbol{P}^r)$ denote the support of $\boldsymbol{P}^r$ i.e., $\mathrm{supp}(\boldsymbol{P}^r) = \{i \mid P^r(i) - P^r(i+1) > 0\}$.

Lemma 1. *Assume that for each positive integer r, $\mathrm{supp}(\boldsymbol{P}^r)$ is finite and contains some relatively prime integers. Then the equality in (16) is satisfied.*

Proof. Suppose that from some stage k on all the stations play SPELL, the current settings being $(r_n^k, q_n^k), n = 1, \ldots, N$. If some stations are executing step 2 in stage k then either $x^k = 0$, so that in stage $k+1$ all the other stations join in step 2 and the assertion follows trivially, or $x^k > 0$, in which case all the stations execute step 1 in stage $k+1$. Since no station deviates from SPELL, the r-counters are never incremented and remain constant at r_n^k. It follows that $(q_1^l, \ldots, q_N^l)_{l=k,k+1,\ldots}$ is an N-dimensional Markov chain with a finite state space. States where $|\{n = 1, \ldots, N \mid q_n^l > Y\}| \leqslant M$ are absorbing (all the stations enter step 2). Moreover, they are accessible from all the other states, rendering the latter transient. Indeed, prior to absorption the value q_n^k at station n returns with positive probability after any number of stages of the form $\sum_{i \in \mathrm{supp}(\boldsymbol{P}^{r_n^k})} l_i \cdot i$, where l_i are nonnegative integers. By Fact 1,

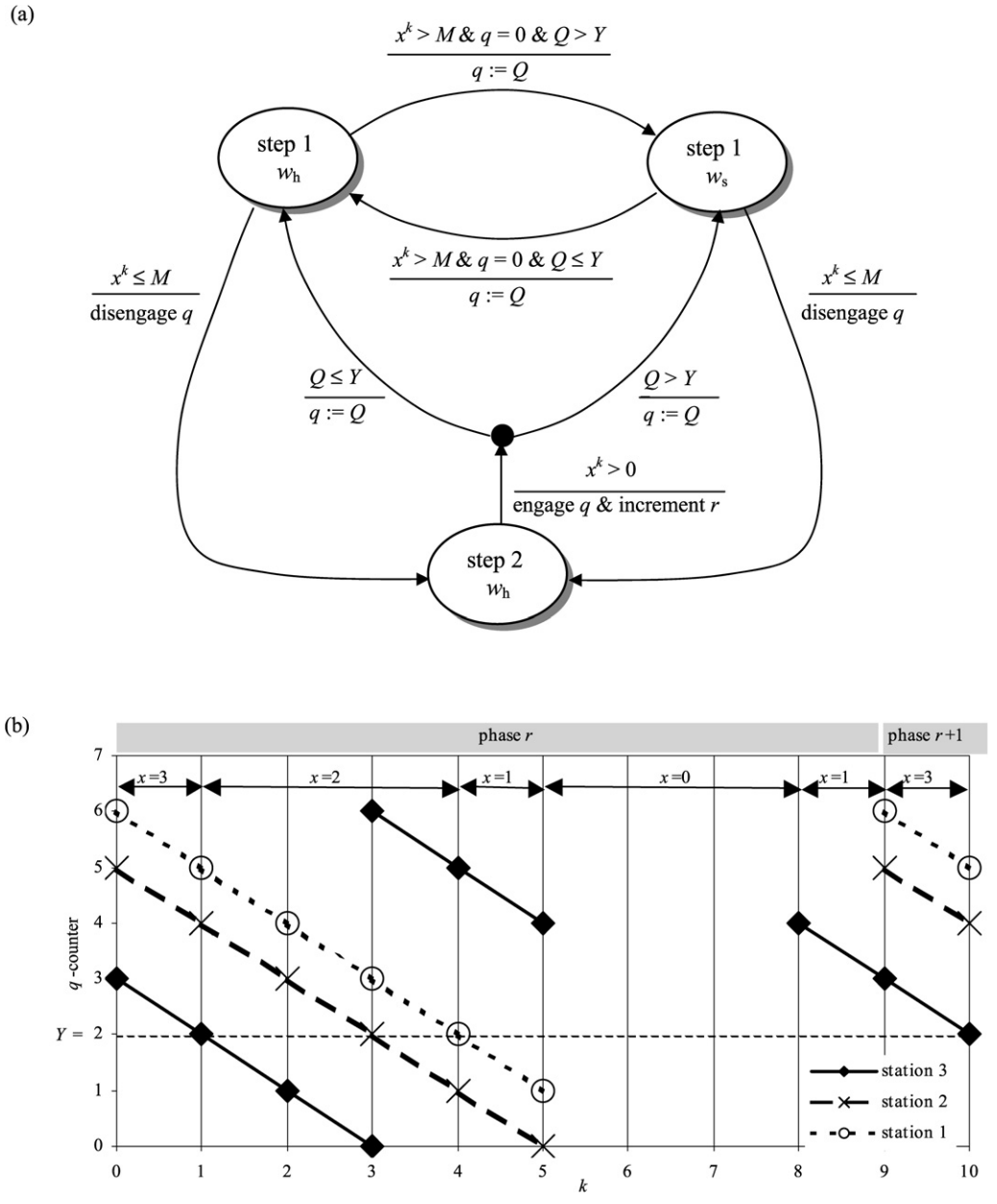


Fig. 4. SPELL operation; (a) state transition diagram, (b) simple scenario in the presence of a deviator.

the set of such numbers includes all consecutive integers above a certain threshold. Hence, for a large enough K, the transition from $(q_1^k, \ldots, q_N^k)$ to any $(q_1^{k+K}, \ldots, q_N^{k+K})$ follows whenever each q_n^k has returned after $K - (q_n^k - q_n^{k+K})$ stages i.e., occurs with positive probability. Let the random variable $S(q_1^k, \ldots, q_N^k)$ represent the number of stages to absorption, given the settings in stage k. Then by Fact 2, $\Pr[S(q_1^k, \ldots, q_N^k) \leqslant s]$ tends to one as s increases. The proof concludes by noting that $E_{\mu(\sigma_n, \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi})} b_n^k = b_{\mathrm{h}}(N, 0) \cdot \Pr[S(q_1^k, \ldots, q_N^k) \leqslant s] + \bar{b} \cdot (1 - \Pr[S(q_1^k, \ldots, q_N^k) \leqslant s])$, where $\bar{b}$ is bounded. □

To verify the right part of (16) i.e., that the strategy profile all-SPELL is a subgame perfect NE of the repeated CSMA/CA game, assume that station n (say) is a deviator i.e., $\sigma_n = \sigma' \neq \text{SPELL}$, while $\sigma_m = \text{SPELL}$ for $m \neq n$. Any

deviation from SPELL causes the other stations to increment their r-counters. If this happens only finitely many times then the assertion follows from the previous lemma, so assume otherwise i.e., that station n is a "persistent deviator".

Lemma 2. *Assume that for each positive integer i, $P^r(i)$ increases with r and $\lim_{r\to\infty} P^r(i) = 1$. Then the inequality in (16) is satisfied.*

Proof. From the proof of Lemma 1 and from Fact 1 it follows that with the r-counters fixed, the number of stages before entering step 2 is finite with probability one: the state for which $|\{m = 1, \ldots, N \mid m \neq n \text{ and } q_m^l > Y\}| = 0$ is accessible from all the other states; with a single "persistent deviator" and $M \geqslant 1$ this means $|\{n = 1, \ldots, N \mid q_n^l > Y\}| \leqslant M$, which implies an absorbing state under all-SPELL. Thus the play undergoes infinitely many r-counter increments, and so by our assumption, for any i and $\varepsilon > 0$ there exists an $\bar{r}(i)$ such that $P^{\bar{r}(i)}(Y+i) > \sqrt[N-1]{1-\varepsilon}$. Let the random variable $\bar{k}$ represent the stage in which the $N-1$ SPELL stations increment their r-counters for the $\bar{r}$th time, and pick any $k > \bar{k}$. Then with probability at least $\vartheta(i) = \sum_{j=1}^{\infty} \Pr[k - \bar{k} = j][P^{\bar{r}(i)}(Y+j)]^{N-1}$ all the SPELL stations still select w_s in stage k. If station n also selects w_s to maximize its payoff (cf. (12)) then $E_{\mu(\sigma_n, \boldsymbol{\sigma}_{-n}; \boldsymbol{\pi})} b_n^k = b_s(N,N) \cdot \vartheta(i) + \bar{b} \cdot [1 - \vartheta(i)]$, where $\bar{b}$ is bounded. By taking a sufficiently large i one ensures that $\vartheta(i)$ becomes arbitrarily close to $1 - \varepsilon$. Recalling (13) concludes the proof. □

Lemmas 1 and 2 yield the following proposition.

Proposition 4. *For $\sigma^* =$ SPELL to satisfy the equality and inequality in (16) it suffices that, respectively,* (i) *for each positive integer r,* $\text{supp}(\boldsymbol{P}^r)$ *is finite and contains some relatively prime integers, and* (ii) *for each positive integer i, $P^r(i)$ increases with r and $\lim_{r\to\infty} P^r(i) = 1$.*

Since the sufficient conditions for (16) are in terms of $\boldsymbol{P}^r$ only, neither M nor Y turns out to be critical to the correctness of SPELL. This leaves room for performance tuning, cf. Section 5.4.

5.3. Modified SPELL

With $w_{n,\min} = 1$ excluded, all-w_s is a unique NE of the CSMA/CA game. Is it reasonable to launch a backoff attack by not invoking the backoff scheme at all i.e., selecting $w_n = w_g = \langle 1, 0\rangle$? Clearly, this would leave all stations besides n with a zero success rate. Station n would land 100% provided that it were the only one to select $\langle 1, 0\rangle$ (hence the subscript "g" for greedy); otherwise it too would get zero. Suppose that the payoffs, now denoted b', reflect not only the success rates, but also transmission cost. Let this cost be negligible except when a station is not the only one to select w_g (i.e., spends all the power on frame collisions), in which case it perceives a "success rate" of $b_C < 0$. Suppose that x, y and $N - x - y$ stations select w_s, w_g, and w_h, respectively. Then $b'_n = b_n$ if $y = 0$; otherwise $b'_n = 0$ if $w_n = w_h$ or $w_n = w_s$, $b'_n = 100\%$ if $w_n = w_g$ and $y = 1$, and $b'_n = b_C$ if $w_n = w_g$ and $y > 1$. Taking $W' = \{w_g, w_s, w_h\}$ we redefine the CSMA/CA game as $(\{1, \ldots, N\}, W', b')$. We shall refer to it as the *ternary CSMA/CA game* as opposed to the *binary CSMA/CA game* discussed earlier.

We see that the ternary game is no longer a Prisoners' Dilemma: any action profile with $y = 1$ (and no other) is a NE. Such asymmetric action profiles, however, are not as compelling as is the unique all-w_s NE in the original game. Consider that the stations may seek a best reply to their beliefs as to the opponents' imminent play; the outcome of the game then depends on the stations' sophistication. For example, first-order sophistication might consist in selecting a best reply to the opponents' best replies to the current profile, rather than to the current profile itself (see [16] for a more systematic exposition and generalization). For a given action profile $(w_n, \boldsymbol{w}_{-n})$, denote by $O^{BR}(\boldsymbol{w}_{-n})$ the set of opponent profiles $\boldsymbol{v}$ in which $v_m \in BR(\boldsymbol{w}_{-m})$ for $m \neq n$ i.e., the opponents have selected best replies to the current action profile. A *first-order sophistication equilibrium* (1SE) is any action profile $\boldsymbol{w}$ in which $w_n \in \bigcup_{v \in O^{BR}(\boldsymbol{w}_{-n})} BR(\boldsymbol{v})$ for all $n = 1, \ldots, N$. While in the original game the only 1SE coincides with the NE, in the present game the set of equilibria is much larger: any action profile is a 1SE. This shows in particular that a strategy coping with possible selections of w_g must not be simply a replica of SPELL with $W = \{w_g, w_h\}$, since w_s is likely to be played too.

For the ternary game we propose to modify SPELL as follows. First, we argue that a station m selecting $w_m^k = w_h$ can distinguish the cases $x^k + y^k = 0$ and $x^k + y^k > 0$ at the end of stage k. Likewise, if $w_m^k = w_s$ then the cases $y^k > 0$, ($y^k = 0$ and $x^k \leqslant M$), and ($y^k = 0$ and $x^k > M$) can be distinguished, and if $w_m^k = w_g$ then the cases $y^k = 1$

and $y^k > 1$ can be distinguished. The distinction is based on the observed b_m^k and b_Σ^k with some "fuzzy" levels defined for each:

- $b_m^k =$ "> 0" or "≈ 0", as separated by the discrepancies between $b_\mathrm{h}(N, 0)$ and $b_\mathrm{h}(N, x)$ with $x > 0$, and between $b_\mathrm{s}(N, x)$ and $b_\mathrm{h}(N, x)$ with $x > 0$ (both discrepancies are visible in Table 2 and occur regardless of N),
- $b_\Sigma^k =$ "high", "low", or "none", as separated by the discrepancy between the total throughput corresponding to $x \leqslant M$ and $x > M$, and the elevation of the latter throughput above zero (this is also visible in Table 2).

Moreover, even under assumption 2 of Section 2, station m can easily recognize the presence of occasional frame collisions in the medium (for RTS/CTS access, a long uninterrupted transmission sensed on the medium indicates a successful DATA frame, therefore short transmissions not followed by a successful DATA frame indicate colliding RTS frames; for basic access, a long transmission not followed by a short one after a SIFS period indicates a colliding DATA frame not followed by an ACK frame). This information can be translated into x^k and y^k as follows:

- If $w_m^k = w_\mathrm{h}$ then the cases $x^k + y^k > 0$ and $x^k + y^k = 0$ are distinguishable as they correspond to $b_m^k =$ "≈ 0" and "> 0", respectively. Moreover, $b_m^k =$ "≈ 0" and $b_\Sigma^k =$ "none" indicate $y^k > 1$; $b_m^k =$ "≈ 0" and $b_\Sigma^k =$ "high" in the absence of frame collisions indicate $y^k = 1$; these same values in the presence of frame collisions indicate $y^k = 0$ and $0 < x^k \leqslant M$; finally, $b_m^k =$ "≈ 0" and $b_\Sigma^k =$ "low" indicate $y^k = 0$ and $x^k > M$.

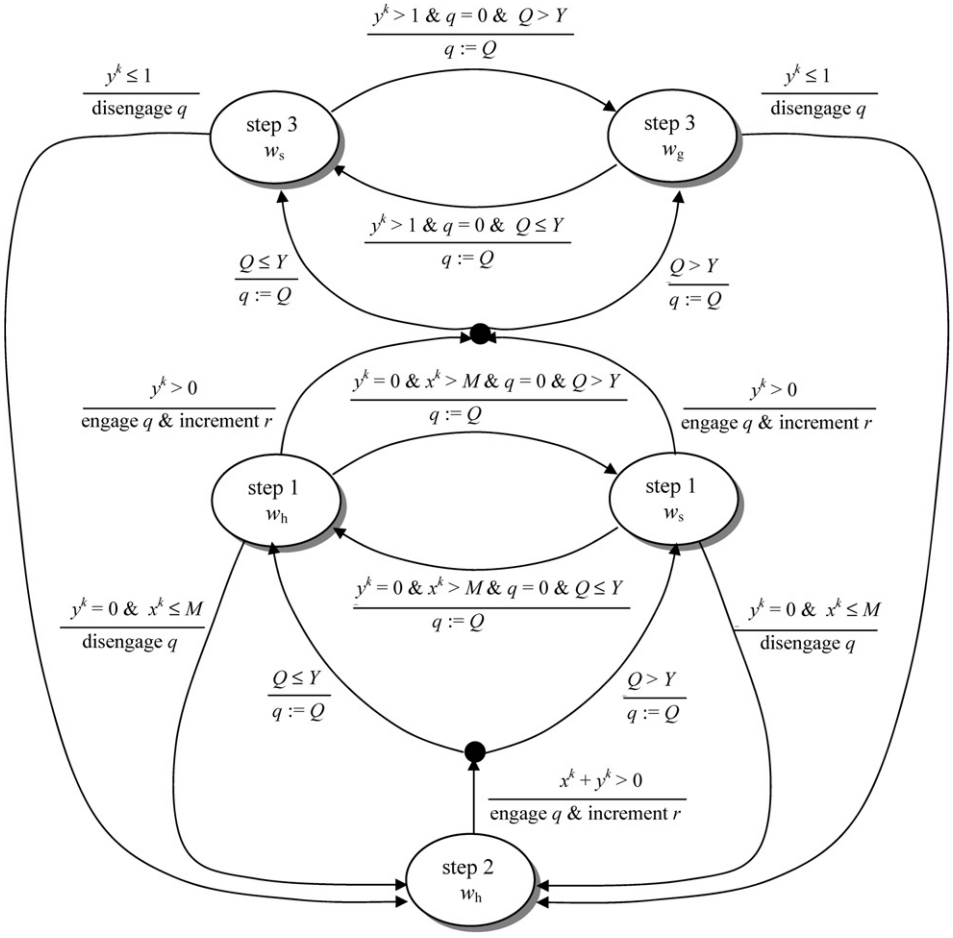


Fig. 5. State transition diagram for modified SPELL.

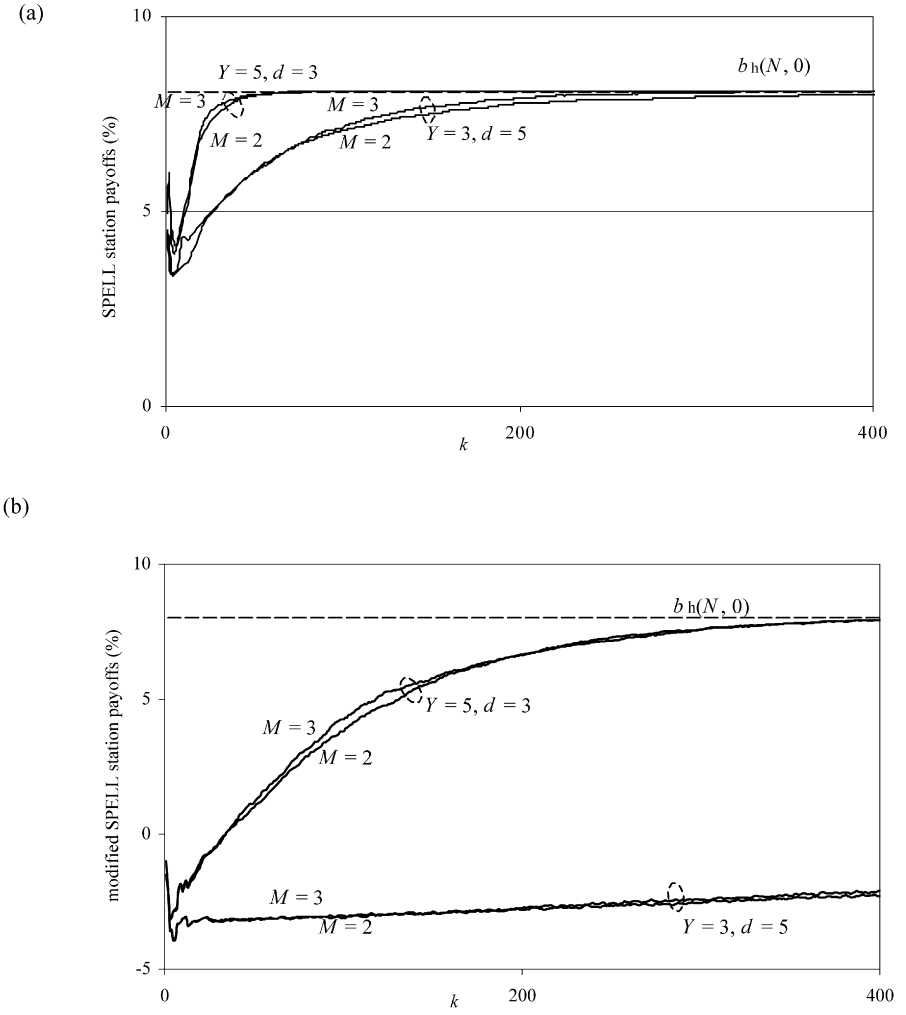


Fig. 6. Convergence to "live-and-let-live"; (a) SPELL, (b) modified SPELL.

- If $w_m^k = w_s$ then $b_m^k =$ "≈ 0" indicates $y^k > 0$; $b_m^k =$ "> 0" and $b_\Sigma^k =$ "high" indicate $y^k = 0$ and $0 < x^k \leqslant M$; finally, $b_m^k =$ "> 0" and $b_\Sigma^k =$ "low" indicate $y^k = 0$ and $x^k > M$.
- If $w_m^k = w_g$ then $b_m^k =$ "≈ 0" indicates $y^k > 1$ and $b_m^k =$ "> 0" indicates $y^k = 1$.

Having initialized r and engaged q, modified SPELL performs steps 1 through 3 below. They are similar to those of SPELL except that in step 1, w_s is selected when $q > Y$ and w_h otherwise, whereas in step 3, w_g is selected when $q > Y$ and w_s otherwise.

1) play out successive spells using q and $\boldsymbol{P}^r$ until either ($y^k = 0$ and $x^k \leqslant M$), whereupon disengage q and go to step 2, or $y^k > 0$, whereupon engage q, increment r, and go to step 3;
2) play honestly until $x^k + y^k > 0$, whereupon engage q, increment r, and go to step 1;
3) play out successive spells using q and $\boldsymbol{P}^r$ until $y^k \leqslant 1$, whereupon disengage q and go to step 2.

The per-stage state transition diagram is shown in Fig. 5. Again, if no station deviates from modified SPELL then step 2 is ultimately executed. In step 1, detection of a station selecting w_g brings about a painful punishment: all SPELL stations enter step 3 and toggle between w_g and w_s until $y^k \leqslant 1$, which may take quite long to happen. Like SPELL, modified SPELL satisfies (16); the proof is similar to that in Section 5.2.

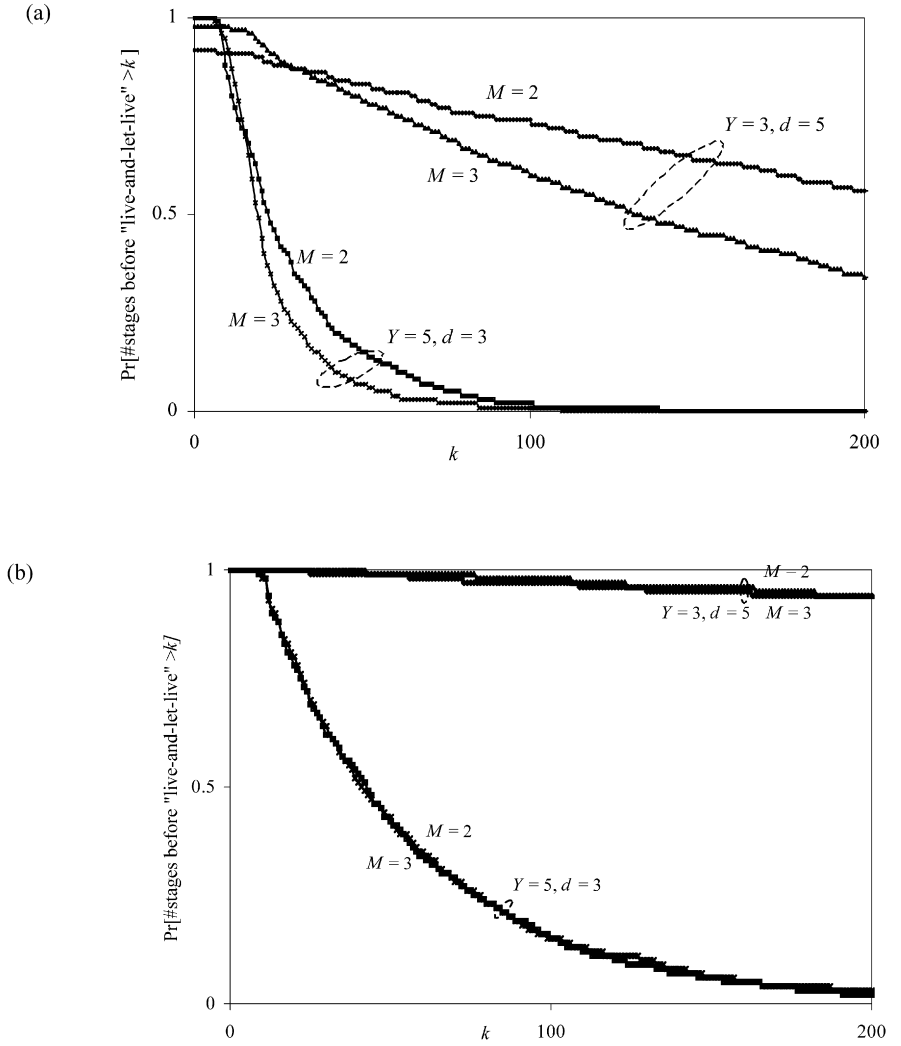


Fig. 7. Distribution of the number of stages before "live-and-let-live"; (a) SPELL, (b) modified SPELL.

5.4. Performance

Sample payoff trajectories ($E_{\mu(\sigma_n,\boldsymbol{\sigma}_{-n};\boldsymbol{\pi})}b_n^k$ vs. k) produced by SPELL and modified SPELL have been obtained via Monte Carlo simulation to illustrate the validity of (16). $N = 10$ and $b_C = -5\%$ were fixed, and stage payoffs for $y = 0$ were taken from Table 2. The probability distributions $\boldsymbol{P}^r$ were uniform over $\{1, \ldots, D^r\}$, with $D^r = D^0 + r \cdot d$. For each station, D^0 was drawn from the range 3..20. Each of the depicted curves emerged after averaging over 1000 runs with the same initial q-counter settings.

Figs. 6(a) and 6(b) illustrate convergence to $b_{\mathrm{h}}(N, 0) = 8.1\%$ in the binary and ternary game in the absence of deviators from SPELL and modified SPELL, respectively. The initial settings were chosen at random (with equal number of stations executing each step of SPELL or modified SPELL); this imitates the effect of an arbitrary play path prior to the start of simulation. It is visible both for the binary and ternary game that the combination of Y and d is far more critical to the speed of convergence than M. Taking Y too small and d too large brings about a long initial punishment for what is perceived as deviations (e.g., when $x^k > 0$ while the q-counter is disengaged at SPELL stations, or when $x^k + y^k > 0$ while the q-counter is disengaged at modified SPELL stations), and what in fact is the impact of the initial settings. This leads to slow convergence to $b_{\mathrm{h}}(N, 0)$, especially for modified SPELL on account of occasional negative payoffs b_C and since the condition of leaving step 3 is equivalent of $M = 1$ in SPELL. Figs. 7(a)

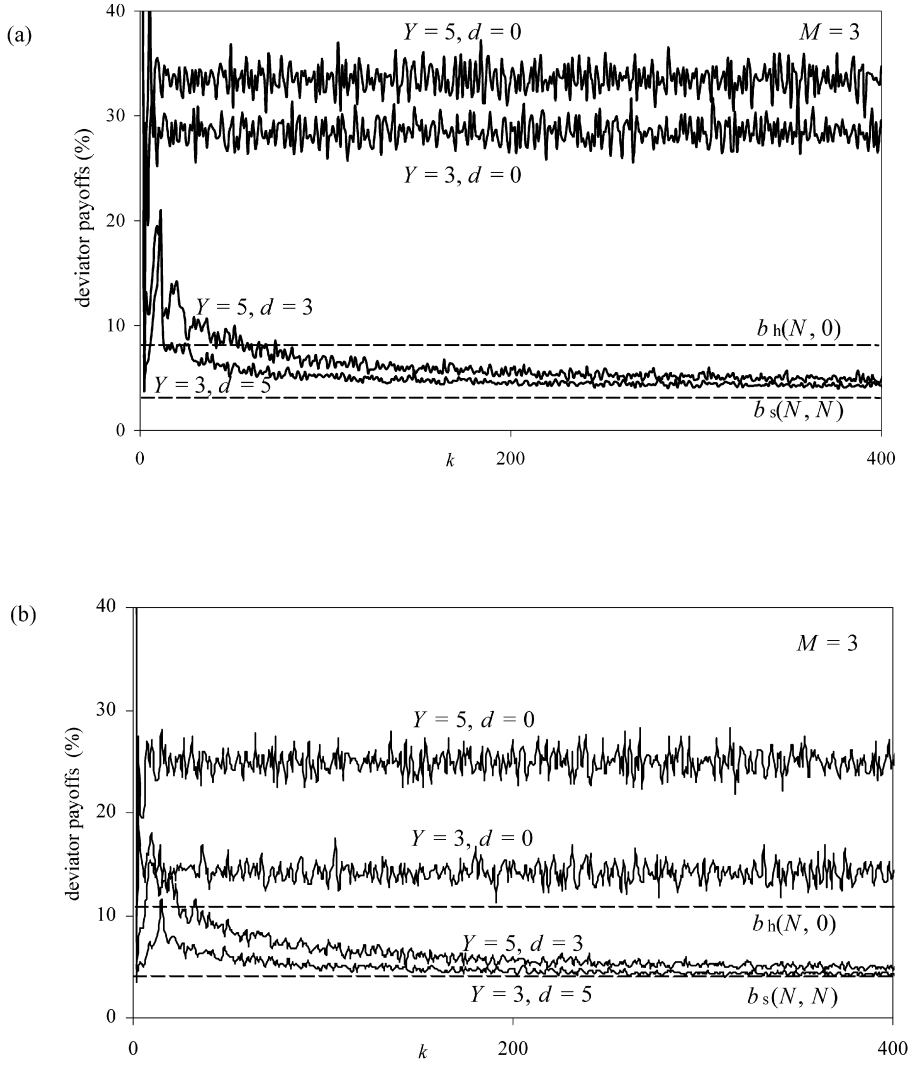


Fig. 8. Single "persistent deviator" performance against (a) SPELL, (b) modified SPELL.

and 7(b) depict complementary probability distribution functions of the number of stages before a "live-and-let-live" scenario sets in.

In Figs. 8(a) and 8(b) one station, say n, persistently deviates from SPELL in the binary game, and from modified SPELL in the ternary game, respectively, while the other stations initially execute step 2. To upper bound the utility of a conceivable deviator strategy, we have experimented with a "good reply" to SPELL that relies on ideal prediction, *prior* to stage k, of the opponent profile in stage k. The deviator selects $w_n^k = w_\mathrm{h}$ when exactly M other stations are to select w_s, and $w_n^k = w_\mathrm{s}$ otherwise. That is, while noticing that w_s always brings higher payoffs than w_h, the deviator will not prevent entering step 2 with a view of landing the highest possible success rate $b_n = b_\mathrm{s}(N, 1)$ in the next stage. Such a strategy is naturally unrealistic unless station n is capable of immediate estimation of throughput at the beginnings of successive stages. Similarly, a "good reply" to modified SPELL selects w_g when all the other stations are to select w_h; otherwise always selects w_s except when no other station is to select w_g, and M or less are to select w_s, in which case it selects w_h. That is, the deviator selects w_g sparingly for fear of rapid detection and punishment, and again will not prevent entering step 2 with a view of landing $b'_n = 100\%$ in the next stage.

That such deviator strategies work well against strategies less smart than SPELL or modified SPELL is demonstrated by the $d = 0$ curves: against a "deficient" SPELL with $d = 0$ (i.e., with the r-counter never incremented), the deviator achieves a stable success rate of 30% to 35% depending on Y i.e., four times the fair success rate $b_\mathrm{h}(N, 0)$.

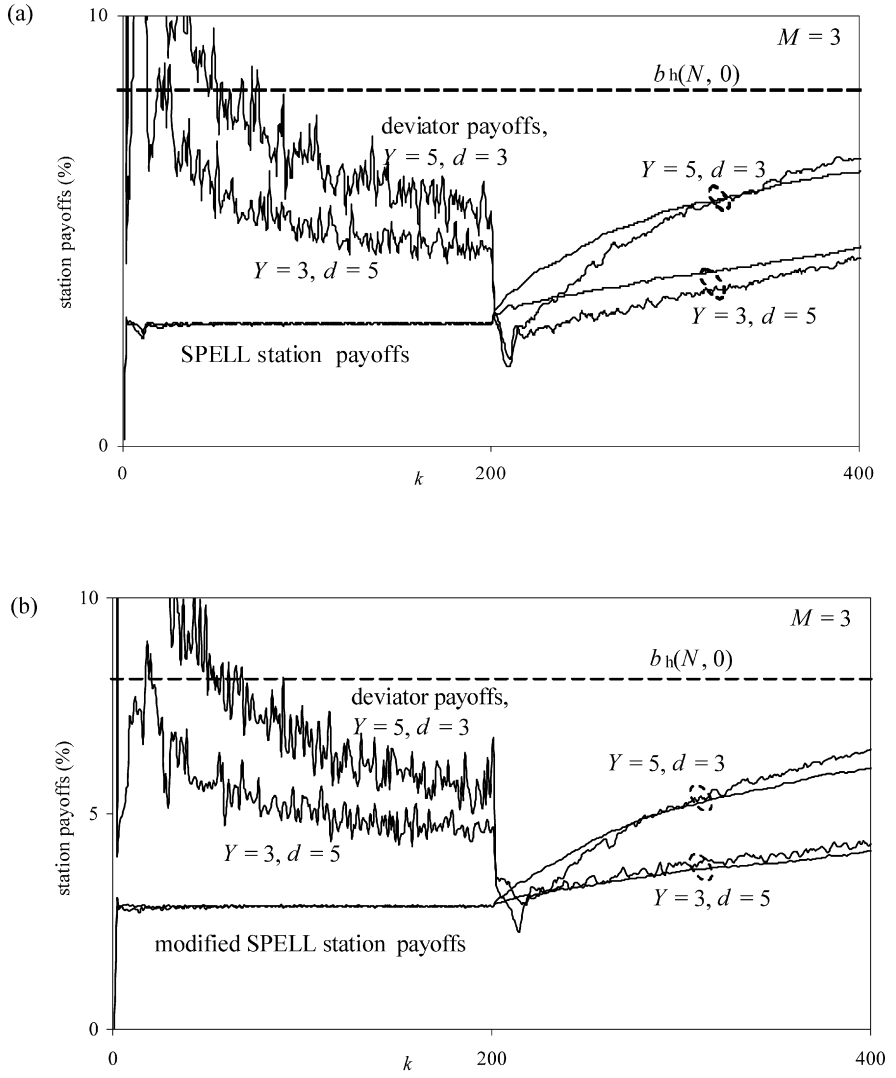


Fig. 9. Single deviator reverting after stage 200 to (a) SPELL, (b) modified SPELL.

Against a "deficient" modified SPELL the deviator success rate reaches 15% or 25% depending on Y, a two- to three-fold markup compared with $b_{\mathrm{h}}(N, 0)$. Yet when $d > 0$, the deviator ultimately fares much worse than it would if playing SPELL or modified SPELL, its average stage payoffs approaching $b_{\mathrm{s}}(N, N) = 3.1\%$ (more rapidly for modified SPELL as a result of occasional negative payoffs b_C). Note that the punishment becomes more prompt and severe with a smaller Y and larger d, revealing a tradeoff between punishment and convergence to $b_{\mathrm{h}}(N, 0)$.

Finally, Figs. 9(a) and 9(b) illustrate the idea of a subgame perfect NE: one station plays the above deviator strategy up to stage 200 and subsequently reverts to SPELL and modified SPELL, respectively. The average stage payoffs then asymptote to $b_{\mathrm{h}}(N, 0)$ (slightly more slowly for modified SPELL) and the live-and-let-live scenario sets in. Note that by stage 200 the deviator will have realized the benefits of reverting to SPELL or modified SPELL.

6. Conclusion

We have proposed and studied a strategy against backoff attacks in wireless ad hoc LANs, in a simplified form where the configuration of the backoff scheme at each station is restricted to greedy, selfish and honest. Using a fairly accurate performance model with stations' success rates regarded as payoffs we have shown that a noncooperative CSMA/CA game then arises with a payoff structure characteristic of a Prisoners' Dilemma. The fact that the unique

NE of such a game is inefficient and that the success rates decrease as the number of attackers increases underlies a simple strategy for the repeated CSMA/CA game, called SPELL. Assuming that the stations are rational players and wish to maximize a long-term utility, SPELL deters a single attacker by preferring greedy or selfish play, yet at any time retains the ability to end up in a live-and-let-live scenario with all the stations selecting the honest configuration. It is worth noting that SPELL can be implemented in the network adapter software without affecting the IEEE 802.11 MAC standard.

Among the issues not addressed in this paper is the ability of SPELL to deter multiple attackers. It seems obvious that a simultaneous backoff attack by multiple stations can only be beneficial if some coordination between them exists. This is not unthinkable and deserves further research.

Acknowledgements

This work was supported in part by the US Air Force Office of Scientific Research under Grant FA8655-04-1-3074 and in part by the ministry of Education and Science, Poland, under Grant 1599/T11/2005/29.

References

[1] E. Altman, R. El Azouzi, T. Jimenez, Slotted ALOHA as a game with partial information, Computer Networks 45 (2004) 701–713.
[2] E. Altman, A. Kumar, D. Kumar, R. Venkatesh, Cooperative and non-cooperative control in IEEE 802.11 WLANs, INRIA Tech. Rep. 5541, 2005.
[3] J. Bellardo, S. Savage, 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions, in: Proc. USENIX Security Symposium, 2003.
[4] G. Bianchi, Performance analysis of the IEEE 802.11 distributed coordination function, IEEE J. Selected Areas Commun. SAC-18 (2000) 535–547.
[5] M. Cagalj, S. Ganeriwal, I. Aad, J.-P. Hubaux, On selfish behavior in CSMA/CA networks, in: Proc. IEEE INFOCOM 2005, Miami, FL, 2005.
[6] A.A. Cardenas, S. Radosavac, J.S. Baras, Detection and prevention of MAC layer misbehavior in ad hoc networks, Univ. of Maryland Tech. Rep. ISR TR 2004-30, 2004.
[7] Z. Fang, B. Bensaou, Fair bandwidth sharing algorithms based on game theory frameworks for wireless ad-hoc networks, in: Proc. IEEE INFOCOM 2004, Hong Kong, 2004.
[8] W. Feller, An Introduction to Probability Theory and its Applications, J. Wiley and Sons, 1966.
[9] D. Fudenberg, J. Tirole, Game Theory, MIT Press, 1991.
[10] IEEE Standard for Information Technology—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ISO/IEC 8802-11, 1999.
[11] V. Knoblauch, Computable strategies for repeated Prisoner's Dilemma, Games and Economic Behavior 7 (1994) 381–389.
[12] C.E. Koksal, H. Kassab, H. Balakrishnan, An analysis of short-term fairness in wireless media access protocols, in: Proc. ACM SIGMETRICS, Santa Clara, CA, 2000.
[13] J. Konorski, Multiple access in ad-hoc wireless LANs with noncooperative stations, in: Lecture Notes in Computer Science, vol. 2345, Springer-Verlag, 2002, pp. 141–1146.
[14] P. Kyasanur, N.H. Vaidya, Detection and handling of MAC layer misbehavior in wireless networks, in: Proc. Int. Conference on Dependable Systems and Networks, 2003.
[15] A.B. MacKenzie, S.B. Wicker, Game theory and the design of self-configuring, adaptive wireless networks, IEEE Comm. Magazine 39 (2001) 126–131.
[16] P. Milgrom, J. Roberts, Adaptive and sophisticated learning in normal form games, Games and Economic Behaviour 3 (1991) 82–100.
[17] O. Queseth, Cooperative and selfish behaviour in unlicensed spectrum using the CSMA/CA protocol, in: Proc. Nordic Radio Symposium, 2004.
[18] M. Raya, J.-P. Hubaux, I. Aad, DOMINO: A system to detect greedy behavior in IEEE 802.11 hotspots, in: Proc. MobiSys Conference, 2004.
[19] R. Rom, M. Sidi, Multiple Access Protocols Performance and Analysis, Springer-Verlag, 1991.
[20] W. Szpankowski, Average Case Analysis of Algorithms on Sequences, J. Wiley and Sons, 2001.
[21] G. Tan, J. Guttag, The 802.11 MAC protocol leads to inefficient equilibria, in: Proc. IEEE INFOCOM 2005, Miami, FL, 2005.
[22] H. Thorisson, Coupling, Stationarity, and Regeneration, Springer-Verlag, 2000.
[23] S.H. Wong, I.J. Wassell, Application of game theory for distributed dynamic channel allocation, in: Proc. 55th IEEE Vehicular Technology Conference, 2002.
[24] X. Yao, Evolutionary stability in the n-person iterated Prisoners' Dilemma, BioSystems 39 (1996) 189–197.
[25] E. Ziouva, T. Antonakopoulos, CSMA/CA performance under high traffic conditions: Throughput and delay analysis, Computer Comm. 25 (2002) 313–321.